
Securing Emerging AI Technologies in Offshore Aquaculture
The pinnacle of sustainable farming.
LEARN MORE

About

Aquacultures cultivate a variety of organisms such as fish, crustaceans, mollusks, and algae.

Most offshore operations are considered small-scale, but some larger farms have been making head waves in their implementation of emerging marine technologies, especially in relation to artificial intelligence (AI).

Mowi located in Norway, has partnered with Tidal, a startup originated from Google's Moonshot Factory, to optimize the farm's management and improve operational efficiency.

Tidal has developed **underwater cameras**, **sensors**, and **software** to actively monitor fish.

(Wright; Jadhav et al.; "Salmon Farm, Varangerhalvoya")

Application and Functionality

Machine Vision Cameras with Sensors

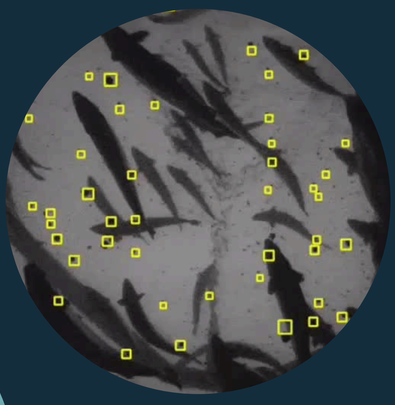
Continuous image collection.

- **Biomass** data derived from the **total number** of fish multiplied by the average **mass** of fish sampled.

Plus, **size** measurements, **sex** identifications, **quality** assessments, **behavior** monitoring, and **feeding** monitoring.

Real-time water reads.

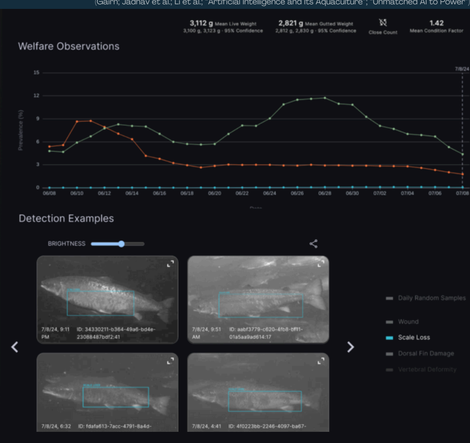
- Sea surface **temperature**, **salinity**, and **oxygen**.

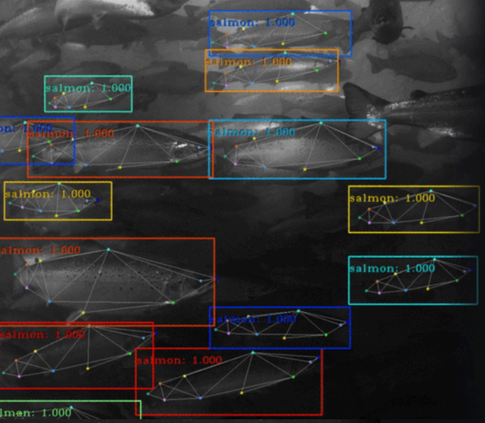


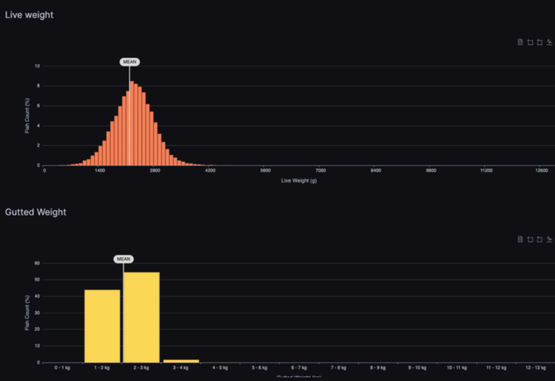
Software System

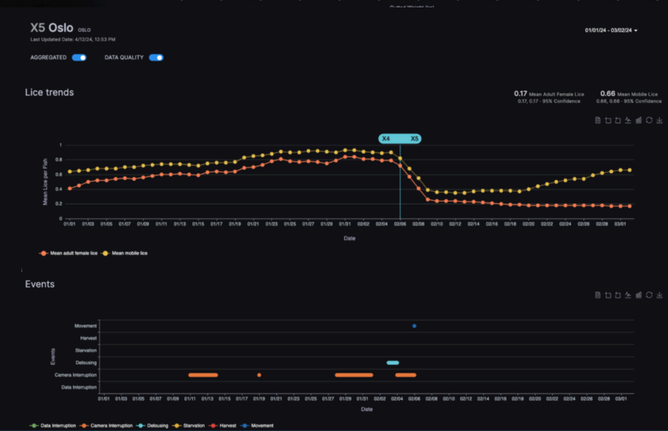
- Time series **modeling**.
- **Machine learning** (ML) predictions.

(Gairn; Jadhav et al.; Li et al.; "Artificial Intelligence and its Aquaculture"; "Unmatched AI to Power")









Cybersecurity Risks

The digital shift demands a steep **learning curve** for farmers used to simpler methods, and poses a risk for insider threats of exposed credentials and compromised systems.

Tidal's AI infrastructure consists of data-gathering devices, connectivity gateways, and a Google Cloud platform.

Due to these **interconnected systems**, cyber-attacks can have a greater, lasting impact on an aquaculture. Allowing attackers to gain control over a larger surface area.

This interconnectivity challenge coupled with the technical expertise required to run and maintain Tidal's infrastructure, leaves aquacultures at high risk for cyber-attacks.

AI Security Risk Overview

Broadened attack surface: AI systems often rely on complex, distributed architectures involving cloud services, APIs and third-party integrations, all of which can be exploited.

Injection attacks: Threat actors manipulate training data or prompt inputs to alter AI behavior, leading to false predictions, biased outputs or malicious outcomes.

Data theft and leakage: AI systems process vast amounts of sensitive data; unsecured pipelines can result in breaches or misuse.

Model theft: Threat actors can reverse-engineer models or extract intellectual property through adversarial methods.

(Huang; Unger; "A Person Riding a Motorboat"; "Pile of Fresh Silver"; "Unmatched AI to Power")

Solving the Security Challenges of AI

TRAINING | API SECURITY | COMPLIANCE

ZERO-TRUST | HARDENING | MONITORING

Employee Training

Incident response training:
- Cybersecurity Information Systems Architecture (CISA) offers Incident Response training courses, addressing offensive and defensive views.

Workforce training:
- CISA offers Professional Development training courses.
- Competitions and games can encourage players to practice, hone cybersecurity skills, and build confidence in a controlled, real-world environment.
- Certifications allow employees to validate their knowledge.

SOLUTIONS

Zero-Trust Framework

- **Authenticate** and **authorize** all available data points.
  - Authenticate to verify user and application identities.
  - Authorize to control access to specific resources.
  - Phishing-resistant multifactor authentication (MFA) should be enforced at the application layer.
  - Employ centralized identity management systems that can be integrated with applications and platform.
- Utilize **least privilege access** control.
  - When authorizing user access to resources, consider at least one device-level signal, with identity information about the authenticated user.
- **Assume breach**.
  - Minimize blast radius and segment access.
  - Verify end-to-end encryption.
  - Use analytics to get visibility, drive threat detection, and improve defenses.

Pillars defined by CISA:
- Identity, devices, networks, applications, and data.

API Security

- Authentication and authorization methods.
  - **OAuth 2.0:** Delegates authentication, allowing third-party applications to access resources without sharing user credentials.
  - **API Keys:** Offers simpler authentication for less sensitive use cases.
  - **JWT (JSON Web Tokens):** Enables secure transmission of data between parties.
- Implement **data encryption**.
  - Prevents eavesdropping and tampering as data moves through APIs and ensures stored data is unusable even if attackers do manage to compromise their data stores.
- Conduct **API discovery**.
  - Identifies and catalogs APIs, creates directories, and compiles an inventory.
  - Helps to track API usage, update API specs, and structure APIs.
- **Regularly audit** and **monitor.**
  - Organizations must proactively identify potential vulnerabilities in API designs and implementations to prevent attackers from exploiting them.
  - Continuously monitoring API activity for unusual patterns, suspicious behavior, and potential breaches ensures that teams can rapidly and effectively respond to threats.
- Utilize **rate limiting** and **throttling**.
  - Rate limiting can restrict the number of requests a client can make within a specific timeframe.
  - Throttling can temporarily delay or reject requests when an API is under heavy load.
  - Attackers often abuse and compromise API availability by overwhelming them with requests.
  - Mitigates denial-of-service (DoS) attacks.
- **Validate inputs**.
  - Verifies data sent to an API conforms to predefined formats, data types, and length constraints.
  - Prevents malicious or malformed data from being processed, protects the underlying AI models, and prevents potential system compromises like SQL injection or cross-site scripting (XSS).

SOLUTIONS

Model Hardening

- **Train models with adversarial examples**.
  - Recommendation - quarterly.
  - Conduct after-action reviews upon completion of training, and increase the sophistication of future threat training.
  - Improves resilience against manipulation.
  - Protects from adversarial attacks, attempting to fool models into making incorrect predictions.
- Implement **input validation** and **anomaly detection**.
  - Ensures models are less susceptible to manipulation, maintaining their accuracy and reliability in real-world applications.
- **Encrypt models**.
  - Prevents theft or unauthorized use.
- Use **runtime protection** technologies.
  - Like secure enclaves (i.e. Intel Software Guard Extensions) to protect models during inference.

Continuous Compliance

Follow a governance program structure:
1. **Confirm High Quality Data Use**
   a. "High-quality data" as a term generally means data being used for high-risk AI is material and relevant to the exercise.
2. **Continuous Monitoring**
   a. Ensure there is continuous monitoring, testing, and auditing pre- and post-deployment of the high-risk use of AI.
3. **Risk Assessment**
   a. Perform risk assessments based on the pre-deployment testing, auditing, and monitoring of the AI. This will require close communication with the enterprise AI management team to ensure that the required processes are in place.
4. **Technical Documentation**
   a. Ensure that all required technical documentation and risk mitigation have been implemented based on the continuous monitoring process—all users, licensees, and deployers of AI must do their own testing.
5. **Transparency**
   a. Licensors and licensees of AI will be expected to be fully transparent with end users as to the capabilities and limitations of the AI.
6. **Human Oversight**
   a. Trusted AI legal frameworks intend for there to be a degree of human oversight to correct deviations from expected uses in real time. This may require a human research scientist within the company who would have the ability to adjust the AI model to bring it back into safety parameters.
7. **Fail-Safe**
   a. In the event that AI cannot be restored to approved parameters, there would need to be a fail-safe "kill switch" if remedial mitigation steps cannot be effectuated.

Frequent Monitoring

Implement **automated monitoring tools**.
- These should utilize AI to analyze logs and detect unusual patterns.
- Regularly review logs and perform security audits.
- Invest in tools that can detect AI-specific threats like data poisoning, model drift, and unauthorized API access.
- Similar tools can be found by companies like IBM, SentinelOne, Glasswall and Wiz.

SOLUTIONS

(AEB et al., Jadhav et al., Murphy, "API Security's Role"; "What is Zero Trust")

Ethics and Values

Only 1/3 of fish stocks are fished unsustainably.

Almost 90 percent of the global fish stocks either fully exploited or overfished.

Data sharing efforts within the aquaculture sector can propel the industry forward by improving their operational efficiency, species health, and innovative solutions.

Making aquacultures cyber secure can prevent attacks that have the potential to impact marine health and create detrimental pollution.

Aquaculture technologies can help promote offshore farming and alleviate pressure on wild fish stocks, provide a more sustainable protein source, and support the livelihoods of coastal communities.

(Jadhav et al.; “Sustainable Aquaculture”; “Tidal - X, the Moonshot Factory”)

Works Cited

Badanes, David, et al. “How AI Will Impact Cybersecurity Regulatory and Disclosure Matters.” *NACD*, 11 Mar. 2025, nacdonline.org/all-governance/governance-resources/governance-research/director-handbooks/DH/2025/ai-in-cybersecurity/how-ai-will-impact-cybersecurity-regulatory-and-disclosure-matters/.

Gairn, Louisa. “WWF and Global Salmon Initiative Launch New Feed Risk Assessment Tool.” *We Are Aquaculture*, 25 Mar. 2024, weareaquaculture.com/news/aquaculture/wwf-and-global-salmon-initiative-launch-new-feed-risk-assessment-tool. Accessed 1 Jun. 2025.

Huang, Yo-Ping. “The Artificial Intelligence of Things and Its Aquaculture Applications.” *Global Seafood Alliance*, 3 Feb. 2025, globalseafood.org/advocate/the-artificial-intelligence-of-things-and-its-aquaculture-applications/. Accessed 7 May 2025.

Jadhav, Rajesh, et al. “This Alphabet Spin-off Brings ‘Fishal Recognition’ to Aquaculture.” *IEEE Spectrum*, 7 Apr. 2025, spectrum.ieee.org/aquaculture.

Li, Daoliang, et al. “Review of Various Machine Vision-Based Methods Relating Fish Size and Mass.” *Global Seafood Alliance*, 16 Nov. 2020, globalseafood.org/advocate/nonintrusive-methods-for-fish-biomass-estimation-in-aquaculture-part-1/. Accessed 30 May 2025.

Murphy, Jerald. “How to Secure AI Infrastructure: Best Practices.” *Search Security*, TechTarget, 2025, techtarget.com/searchsecurity/tip/How-to-secure-AI-infrastructure-Best-practices. Accessed 8 May 2025.

Skaug, Martin. “Op-Ed: AI Data Modeling and Nanotechnology Are Innovations Every Farmer Should Be Taking Note Of.” *SeafoodSource*, 4 Sep. 2025, seafoodsource.com/news/aquaculture/ai-data-modelling-and-nanotechnology-are-innovations-every-farmer-should-be-taking-note-of.

Unger, Nitzan. “Harnessing AI in Aquaculture.” *The Fish Site*, 31 Mar. 2025, thefishsite.com/articles/harnessing-ai-in-aquaculture. Accessed 8 May 2025.

Wright, Jamie. “Talking about Farming Fish, Bright Futures and Even Some Failures at the Blue Food Innovation Summit.” *Global Seafood Alliance*, 15 Apr. 2025, globalseafood.org/advocate/talking-about-farming-fish-bright-futures-and-even-some-failures-at-the-blue-food-innovation-summit/. Accessed 7 May 2025.

“A Person Riding a Motorboat Near a Group of People in a White Boat.” *Pexels*, uploaded by Jimmy Ramirez, 3 Dec. 2021, pexels.com/photo/a-person-riding-a-motorboat-near-a-group-of-people-in-a-white-boat-10436682/.

“API Security’s Role in Responsible AI Deployment.” *API Security*, Wallarm, 21 Jan. 2025, lab.wallarm.com/api-securitys-role-in-responsible-ai-deployment/.

“Artificial Intelligence and Its Aquaculture Applications.” *Environment Costal & Offshore*, 4 Feb. 2025, ecomagazine.com/news/fisheries-aquaculture/artificial-intelligence-and-its-aquaculture-/.

“Pile of Fresh Silver Fish.” *Pexels*, uploaded by Engin Akyurt, 1 Nov. 2021, pexels.com/photo/pile-of-fresh-silver-fish-10112459/.

“Salmon Farm, Varangerhalvoya, Soroya, Norway.” *Adobe Stock*, uploaded by Westend61 Video, stock.adobe.com/video/salmon-farm-varangerhalvoya-soroya-norway/358170788?prev_url=detail.

“Sustainable Aquaculture.” *The Ocean Foundation*, 7 Aug. 2010, oceanfdn.org/sustainable-aquaculture/.

“The Surface of the Water is Calm and Clear.” *Pexels*, uploaded by Ahmed, 21 Feb. 2024, pexels.com/video/the-surface-of-the-water-is-calm-and-clear-20349820/.

“Tidal - X, the Moonshot Factory.” *X, the Moonshot Factory*, x.company/projects/tidal/.

“Unmatched AI to Power Data-Driven Decisions.” *TidalX AI*, tidalx.ai/en/product#hardware.

“What is Zero Trust?” *Microsoft Security*, Microsoft, 27 Feb. 2025, learn.microsoft.com/en-us/security/zero-trust/zero-trust-overview.